Journal of Behavioral Informatics
Digital Humanities & Development Research
www.behaviouralinformaticsjournal.info

Vol 6, No 1, March, 2020

Access Control into Examination Halls Using Biometric Technology: A Review

[1]Alao, K. A., [2]Yusuf, Y., [3]Alarape, M. A. & [4]Ndakotsu, A. A.
[1,2,3]Department of Computer Science
[4]Department of Computer Engineering
The Federal Polytechnic, Bida
Bida, Niger State, Nigeria
e-mail: andzeem@yahoo.com, andzeem14@gmail.com
Phone: +2348036318009

ABSTRACT

Access Control into examination halls in most of the higher institutions of learning is a manual approach. This manual approach is paper-based that involves mere display and presentation of various mode of identification such as student's identity card, library card, receipts of payment of school fees, examination photo card. This approach is very ineffective in the sense that it gives room for presentation of fake identification documents, impersonation, and waste of time where there is large population of students to be checked into the examination hall. As a way of ameliorating the aforementioned challenges, biometric technology of different methods has been introduced. This research therefore compiled and reviewed available biometric systems and methods adopted for access control into examination halls in higher institutions of learning. The achievements recorded through these various biometric systems and methods were enumerated and their limitations for further research were identified for the enhancement of the effectiveness of biometric technology for access control into examination halls. This study throws more light on literature review of biometric systems and methods for access control into examination halls for the understanding of prospective researchers in the area.

Keywords: Access Control, Biometric Systems, Examination, Identification, Impersonation.

Journal Reference Format:
Alao, K. A., Yusuf, Y., Alarape, M. A. & Ndakotsu, A. A. (2020): Access Control into Examination Halls Using Biometric Technology: A Review. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 6 . No. 1, Pp 81-94.
Available online at https://www.behaviouralinformaticsjournal.info

1. INTRODUCTION

The advancement in technology has made it possible to adopt several modern approaches for easy verification, identification, and authorization of people into venues and for large-scale identity management by organizations and companies. One of such modern approaches is a biometric technology, which measures the physiological and behavioral characteristics of an individual for purposes of verification, identification, and authorization. Biometrics is the most pertinent means of identifying and authenticating individuals in a reliable and fast way through the use of unique biological characteristics. The term "biometrics" according to Rood and Hornak (2008) as cited in Ogherohwo and Ezeoba (2016) is derived from the Greek words "bio" (life) and "metrics" (to measure). Ekwonwune and Okonkwo (2019) described biometrics as a form of identification and access control used in Computer Science. Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders (Joseph & Lynette, 2010). There are many areas of application of biometric technology, and such areas include and not limited to banking, education, electioneering, security etc. In education, biometric technology is used for lecture attendance monitoring, students' registration, examination attendance, and recently access control into examination hall.

2. AN OVERVIEW OF BIOMETRIC TECHNOLOGY

Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known) and consequently that they belong to a group with certain rights or to a group to be denied certain privileges (Ekwonwune & Okonkwo, 2019). Joseph and Lynette (2010) explained that in a variety of government and private domains, biometric recognition is being promoted as a technology that can help identify terrorists, provide better control of access to physical facilities and financial accounts, and increase the efficiency of access to services and their utilization. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things. Commercially, finger-imaging sensors, whose cost and physical size have been reduced, now appear on many laptop personal computers, hand-held devices, mobile phones, and other consumer devices. The motivations for using biometrics are diverse and often overlap, they include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security.

2.1 Current Approaches to Admittance into Examination Halls

All academic institutions have certain criteria for admitting students into examination hall. Some of them are keeping of the accurate record of attendance at lectures, school fees payments are very important (Ekwonwune & Okonkwo, 2019). In today's higher institutions of learning, verification and authentication of student identity can be easily falsified, thus impersonation becomes rampant in lecture hall or examination hall due to lack of effective measure in carrying out verification process (Oyediran, Wahab, Elegbede & Enegbe, 2018). Access to examination halls in most of the higher institutions of learning is a manual approach. This manual approach is paper-based that involves mere display and presentation of various mode of identification such as student's identity card, library card, receipts of payment of school fees, examination photo card.

2.2 Challenges with the Present Approach and Research Direction

This approach is very ineffective in the sense that it gives room for presentation of fake identification documents, impersonation, and waste of time where there is large population of students to be checked into the examination hall. In order to overcome the above problem, researchers have focused on the use of artificial techniques and use of biometrics, leading to the introduction of different biometric methods. This research therefore compiled and reviewed available biometric systems and methods adopted for access into examination halls in higher institutions of learning. The achievements recorded in the use of these various biometric systems and methods were enumerated and their limitations for further research were identified for the enhancement of the effectiveness of biometric technology for controlled access into examination halls.

3. RESEARCH METHODOLOGY

This study adopted primary method by observation of access control into examination hall, and secondary method with the review of related work and literatures, which includes journals, textbooks, conference proceedings, websites articles, encyclopedia articles. Articles used are within the last one decade with focus on the recent ones.

3.1 Biometric Modalities

According to Joseph and Lynette (2010) a biometric modality is the combination of a biometric trait, sensor type, and algorithms for extracting and processing the digital representations of the trait. When any two of these three constituents differ from one system to the next, the systems are said to have different modalities. For example, infrared facial recognition and iris recognition are different modalities since the trait and the algorithms differ even if the same camera is used. A biometric modality refers to a system built to recognize a particular biometric trait such as face, fingerprint, hand geometry, palm print, iris, voice, signature, gait, and keystroke dynamics (Joseph & Lynette, 2010).

Some common biometric modalities described by Jain, Ross and Prabhakar (2004) are summarized briefly as follows.

(i) **Face:** Static or video images of a face can be used to facilitate recognition. Modern approaches are only indirectly based on the location, shape, and spatial relationships of facial landmarks such as eyes, nose, lips, chin, and so on. Ahmed and Abdulaziz (2017) noted that a camera of some sort (digital, video or thermal) is used to capture the features such as the upper outlines of the eye sockets, the cheekbones, the sides of the mouth, and the location of the nose and eyes. Video facial recognition maps out a number of points on the face or creates a three dimensional image to be used for comparison. The user is usually required to stand a few feet away and most systems are capable of compensating for expressions, glasses, hats and beards. The issue with the use of face trait is time that elapses between enrollment in a system and when recognition is attempted, because facial appearance changes over time. Also, poor lighting can cause problems so most systems will need to be placed in well-lit areas.

(ii) **Fingerprints:** The patterns of ridges and valleys on the "friction ridge" surfaces of fingers have been used in forensic applications for over a century. Friction ridges are formed in uterus during foetal development, and even identical twins do not have the same fingerprints. The recognition performance of currently available fingerprint-based recognition systems using prints from multiple fingers is quite good. Challenges include the fact that large-scale fingerprint recognition systems are computationally intensive, particularly when trying to find a match among millions of references. Also, Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader (O'Gorman, 2001, as cited in Ahmed & Abdulaziz, 2017).

(iii) **Finger Vein Pattern:** It contains vein patterns, which is the networks of blood vessel under the skin of finger. Every human being has unique vein patterns; even the identical twins have different vein patterns. Finger vein patterns have greater significant as compare with other popular biometrics traits (Hashimoto, 2006, as cited in Akintoye, Araoye & Adu, 2018). Apart from spoofing, finger vein pattern offers some certain key advantages over other biometric based authentications in the sense that it does not entail the subject to place his finger in contact with the scanning surface of scanner machine. Thus, there are no hygiene disputes associated with finger vein scanning and it does not leave any latent prints behind. In addition, wet or dry weather does not affect it since it is sub-dermal, and age has no effect on it, which means that the enrolment can be used for the whole lifetime of the subject (Mulyono & Jinn, 2008, as cited in Akintoye *et al.*, 2018).

(iv) **Hand Geometry:** Hand geometry refers to the shape of the human hand, size of the palm, and the lengths and widths of the fingers. Hand geometry involves the analysis and measuring of the hand and fingers (Alotaibi, 2010, as cited in Ahmed & Abdulaziz, 2017). The user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established modalities of biometrics today. It is accurate and fast. Advantages of this modality are that it is comparatively simple and easy to use. However, because it is not clear how distinctive hand geometry is in large populations, such systems are typically used for verification rather than identification. Moreover, because the capturing devices need to be at least the size of a hand, they are too large for devices like laptop computers.

(v) **Palm Print:** This combines some features of fingerprints and hand geometry. Human palms contain ridges and valleys, like fingerprints, but are much larger, necessitating larger image capture or scanning hardware (Jain *et al.*, 2004).

(vi) **Iris:** The iris, the circular coloured membrane surrounding the eye's pupil, is complex enough to be useful for recognition. For iris scanning, a camera is used to record a digital image of the user's iris (Ahmed & Abdulaziz, 2017). The performance of systems using this modality is promising. Although early systems required significant user cooperation, more modern systems are increasingly user friendly.

However, although systems based on the iris have quite good False Match Rate (FMR), the False NonMatch Rate (FNMR) can be high. Further, the iris is thought to change over time, but variability over a lifetime has not been well characterized (Baker, Bowyer & Flynn, 2009).

(vii) **Voice:** Voice directly combines biological and behavioral characteristics. Voice verification uses a microphone-recording device to capture a sample of a user's voiceprint. Measurements of a number of characteristics were taking, including cadence, pitch, and tone (Ahmed & Abdulaziz, 2017). The sound an individual makes when speaking is based on physical aspects of the body (mouth, nose, lips, vocal cords, and so on) and can be affected by age, emotional state, native language, and medical conditions. The quality of the recording device and ambient noise also influence recognition rates.

(viii) **Signature:** Signatures have been accepted as a method of recognition for a long time. According to Ahmed and Abdulaziz, (2017) signature verification involves the use of a special pen, tablet, or both to capture the way a person signs their name. Although the final appearance of the signature is important, a number of other attributes are captured as well (Hernandez, Ortiz, Andaverde & Burlak, 2008, as cited in Ahmed & Abdulaziz, 2017). These include speed, velocity, pressure, angle of the pen as well as the number of times the pen is lifted from the pad. However, extensive experience has also shown that signatures are relatively easy to forge, and also how a person signs his or her name typically changes over time. It can also be strongly influenced by context, including physical conditions and the emotional state of the signer.

(ix) **Gait:** Gait, the manner in which a person walks, has potential for human recognition at a distance and potentially, over an extended period of time. Laboratory gait recognition systems are based on image processing to detect the human silhouette and associated spatiotemporal attributes. Gait can be affected by several factors, including choice of footwear, the walking surface, and clothing. Gait recognition systems are still in the development stage.

(x) **Keystroke:** Keystroke dynamics are a biometric trait that some hypothesize may be distinctive to individuals. Indeed, there is a long tradition of recognizing 'Morse code' operators by their "fists"; the distinctive patterns individuals used to create messages. However, keystroke dynamics are strongly affected by context, such as the person's emotional state, his or her posture, type of keyboard, and so on.

(xi) **Body Odour:** Body odour recognition is a contactless physical biometric that attempts to confirm a person's identity by analyzing the olfactory properties of the human body scent (Olufemi, 2010). The human odour is released from various parts of body and exists in various forms such as exhalation, armpits, urine, stools, farts or feet (Chatchawal, Mario & Teerakiat, (2009) as cited in Oyeleye, Fagbola, Babatunde & Adigun, 2012). Each chemical of the human odour is extracted by the biometric system and converted into a unique data string. The body odour as a biometric identifier has the lowest error rate (15%) in comparison to other biometric identifiers and the advantage lies in the fact that it is impossible to replicate human odour (Inbavalli & Nandhini, 2014).

Figure 1 below shows various biometric modalities that can be used for identification, verification and authorization.

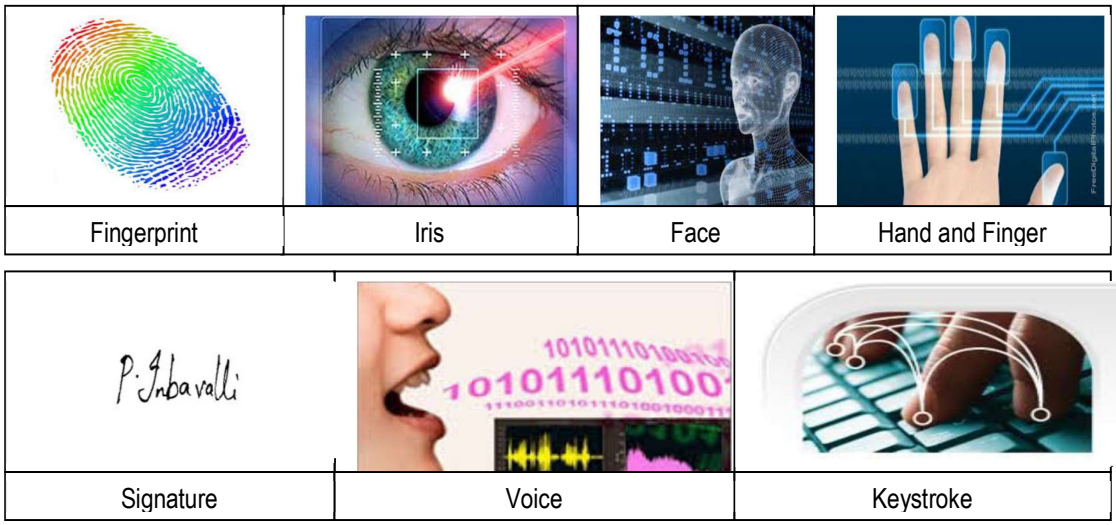

Figure 1: Biometric Modalities
Source: Inbavalli & Nandhini (2014).

Also, figures 2 and 3 below show samples of scanners for capturing biometric traits, such as fingerprints and finger vain.

Figure 2: Samples of Finger Vein and Fingerprint Biometric Access Control Scanner
Source: Danny (2020)

Figure 3: Sample of Finger Vein Biometric Access Control Scanner
Source: Akintoye *et al*., (2018)

3.2 Factors to be Considered When Choosing a Modality

Raphael and Young (1974), as cited in Joseph and Lynette (2010) identified a number of factors that make a physical or a behavioral trait suitable for a biometric application. The following seven factors were taken from an article by (Jain, Bolle & Pankanti, 1999, as cited in Joseph & Lynette, 2010).

(i) **Universality:** Every individual accessing the application should possess the trait.
(ii) **Uniqueness:** The given trait should be sufficiently different across members of the population.
(iii) **Permanence:** The biometric trait of an individual should be sufficiently invariant over time with respect to a given matching algorithm. A trait that changes significantly is not a useful biometric.
(iv) **Measurability:** It should be possible to acquire and digitize the biometric trait using suitable devices that do not unduly inconvenience the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative features.
(v) **Performance:** The recognition accuracy and the resources required to achieve that accuracy should meet the requirements of the application.
(vi) **Acceptability:** Individuals in the target population that will use the application should be willing to present their biometric trait to the system.
(vii) **Circumvention:** The ease with which a biometric trait can be imitated using artifacts, for example, fake fingers in the case of physical traits and mimicry in the case of behavioral traits should conform to the security needs of the application.

3.3 Simple Operations of a General Biometric System

The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). The figure 4 below depicts the operation of a generic biometric system, although some systems will differ in their peculiarities.

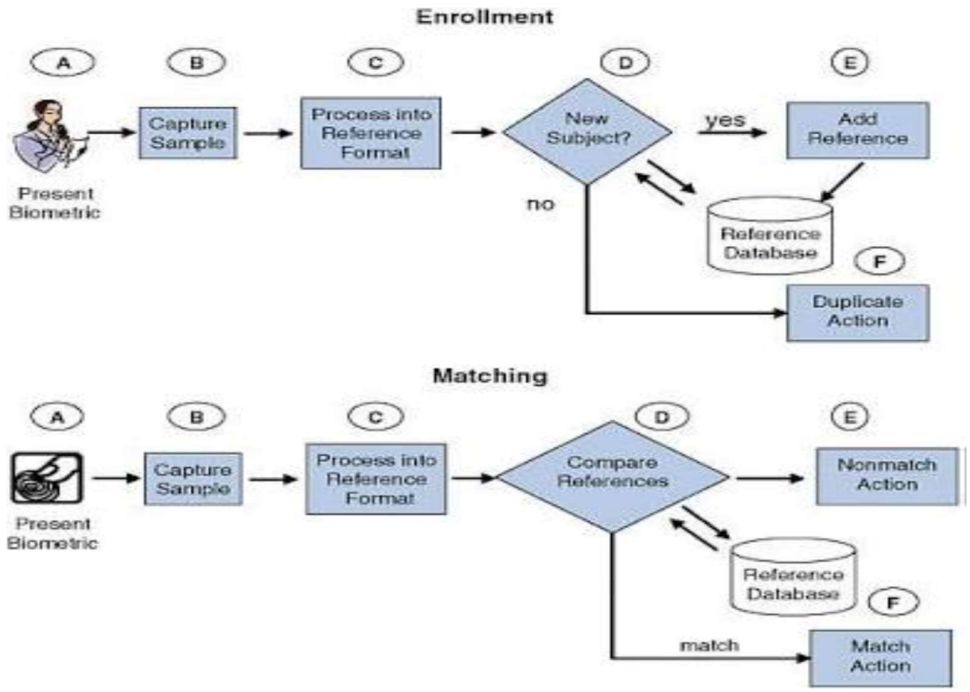

Figure 4: (High-level Model for Enrollment and Matching
Researchgate, n.d, as cited in Ekwonwune & Okonkwo (2019)

The primary components for the operations are "capture" where the sensor collects biometric data from the subject to be recognized; the "reference database" where previously enrolled subjects' biometric data are held; the "matcher" which compares presented data to reference data in order to make a recognition decision and "action" where the system recognition decision is revealed and actions are then undertaken based on that decision (Joseph & Lynette, 2010).

3.4 Use of Multibiometric Modalities

The use of a single biometric modality may not always provide the performance needed from a given system. One approach to improving performance (error rates but not speed) and applications is the use of multibiometrics, which has several forms (Ross & Jain, 2004).

These are as follows.

(i) **Multisensors:** Here, a single modality is used, but multiple sensors are used to capture the data. For example, a facial recognition system might employ multiple cameras to capture different angles on a face.
(ii) **Multiple Algorithms:** The same captured data are processed using different algorithms. For example, a single fingerprint can be processed using minutiae and texture. This approach saves some sensor and associated hardware costs, but adds computational complexity.
(iii) **Multiple Instances:** Multiple instances of the same modality are used. For example, multiple fingerprints may be matched instead of just one, as may the irises of both eyes. Depending on how the capture was done, such systems may or may not require additional hardware and sensor devices.
(iv) **Multisamples:** Multiple samples of the same trait are acquired. For example, multiple angles of a face or multiple images of different portions of the same fingerprint are captured.
(v) **Multimodal:** Data from different modalities are combined, such as face and fingerprint, or iris and voice. Such systems require both hard-ware (sensors) and software (algorithms) to capture and process each modality being used.

3.5 Performance Metrics: Measures of Operational Efficacy

According to Saheed, Hambali, Adeniji and Kadri (2017) the following approach can be used for automated evaluation of the performance of a biometric system.

(i) **True Acceptance Rate (TAR) / True Match Rate (TMR)**: This measures represents the degree that the biometric system is able to correctly match the biometric information from the same person. This measure should be at maximum.
(ii) **False Acceptance Rate (FAR) / False Match Rate (FMR)**: This measure represents the degree or frequency where biometric information from one person is falsely reported to match the biometric information from another person. This measure should be at minimum.
(iii) **True Rejection Rate (TRR) / True Non-Match Rate (TNMR)**: This measure represents the frequency of cases when biometric information from one person is correctly not matched to any records in a database because, in fact, that person is not in the database. This measure should be at maximum.
(iv) **False Rejection Rate (FRR) / False Non-Match Rate (FNMR)**: This measure represents the frequency of cases when biometric information is not matched against any records in a database when it should have been matched because the person is, in fact, in the database. This measure should be at minimum.

3.6 Challenges Associated with The Use of Biometric Technology

There are numerous sources of uncertainty and variation in biometric systems, these include the following as identified by (Joseph & Lynette, 2010).

(i) **Variation within Persons:** Biometric characteristics and the information captured by biometric systems may be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, socio-cultural aspects of the situation in which the presentation occurs, changes in human interface with the system, and so on. As a result, each interaction of the individual with the system (at enrollment, identification, and so on) will be associated with different biometric information. Individuals attempting to thwart recognition for one reason or another also contribute to the inherent uncertainty in biometric systems.

(ii) **Sensors:** Sensor age and calibration, how well the interface at any given time mitigates extraneous factors, and the sensitivity of sensor performance to variation in the ambient environment (such as light levels), all can play a role.

(iii) **Feature Extraction and Matching Algorithms:** Biometric characteristics cannot be directly compared but require stable and distinctive "features" to first be extracted from sensor outputs. Differences in feature extraction algorithms affect performance, with effects sometimes aggravated by requirements for achieving interoperability among proprietary systems.

4. EXAMINATION AND BIOMETRIC TECHNOLOGY

Formal examination can rightly be defined as the assessment of a person's performance, when confronted with a series of questions, problems, or tasks set to him, in order to ascertain the amount of knowledge that he or she has acquired, the extent to which he or she is able to utilize it, or the quality and effectiveness of the skills he or she has developed (Ahmed & Abdulaziz, 2017). Examination is also defined as a formal test of one's knowledge or ability in a particular subject especially by means of answering questions or practical exercises (Benard, 1998, as cited in Ogherohwo & Ezeoba, 2016).

Therefore, it is through examination that students are evaluated or tested to find out the quality and quantity of knowledge they have acquired within a specific period. Thus, examination could be either internal, external, oral, written or both. Continuous assessment scores, terminal, semester, annual or promotion examinations are examples of internal examinations (Benard, 1998, as cited in Ogherohwo & Ezeoba, 2016). Although student's performance in examination may not be the true reflection of their ability, up till now, examination still remains the best tool for an objective assessment and evaluation of what a learner has achieved after a period of schooling/training. In fact, it is one of the most reliable indicators used to determine the extent of students' performance in a given training (Ogherohwo & Ezeoba, 2016).

Examination is a major activity carried out in schools to ascertain how well the students have been able to grasp what had been taught. The instructor/teacher's aim is to see that the learners understand and retain a large portion of what had been taught, the students' major aim is to get high grades (Folaponmile, Okpe & Gwani, 2018). Some learners burn the mid night oil and make a lot of effort in order to understand and acquire high grades, others look for "short cuts" which are usually criminal in nature to acquire high grades. Some students even go to the extent of involving a third party to undertake examinations for them; this is referred to as impersonation.

4.1 Examination Malpractices

Examination malpractice is an illegal act committed by a single student or in collaboration with others like fellow students, parents, teachers, supervisors, invigilators, computer operators or secretarial staff and anybody or group of people before, during, or after examination in order to obtain undeserved marks or grades (Awanbor, 2004, as cited in Ogherohwo & Ezeoba, 2016). According to Olufemi (2010) examination malpractice has been defined as a deliberate wrong doing contrary to official examination rules designed to place a candidate at an unfair advantage or disadvantage.

Examination malpractice has long graduated from the normal giraffing at neighbors‟ work, using key points, notes or textbooks or copying on sheets of papers referred to as “microchips”, or “expo”, or copying on desks or laps also known as “desktop publishing” and “laptop publishing” respectively to a more advanced and more organized system of buying questions from examination bodies or corrupt bank officials or individual entrusted with the safe keeping of examination question papers (Eromosele, 2008, as cited in Olufemi, 2010).

Examination malpractice is not a new phenomenon in Nigeria. The first examination malpractice in Nigeria occurred in 1914 during the Senior Cambridge Local Examination papers which were leaked before the scheduled date of examination (Maduemezia, 1998, as cited in Ogherohwo & Ezeoba, 2016).

Examination malpractice occurs in both internal and external examinations. In short, it has become an epidemic in the nation’s educational system, which needs a prompt attention. The situation of examination malpractice is so embarrassing to the nation that the Federal Military Government in 1984 promulgated Decree 20 to deal with it. Parts of the Decree reads as: “*Any person who fraudulently or with intent to cheat or secure any unfair advantage to himself or any other person or in abuse of his office, produces and sells or buys or otherwise deals with any question paper intended for the examination of persons at any examination or commits any of the offences specified in section 3(2 7) (c) of this Decree, shall be guilty of an offence and on conviction be sentenced to 21 years imprisonment* ” (Ogherohwo & Ezeoba, 2016). Thus, examination malpractice which started at a low trend became more pronounced in 1970, involving persons other than the candidates, since then examination malpractice became more advanced and sophisticated and it has developed to the level where friends can impersonate their friends and sit for an exam for them (Ogherohwo & Ezeoba, 2016). These irregularities have in no doubt posed a vital question on the credibility of the examination system and standard.

4.2 Forms of Examination Malpractices

In recent times, examination malpractice has gone from simple ‘giraffing’ where students occasionally stretch their necks to catch glimpse of what they want to copy from other students scripts to a variety of sophisticated ones (Ogherohwo & Ezeoba, 2016). According to Ahmed and Abdulaziz (2017) year-in-year-out; students come up with new dimensions of examination malpractices. This is the reason why drastic steps must be taken. The instances of examination malpractices vary. They range from impersonation, leakage of questions, tampering with results, and computer fraud to fraudulent practices by invigilators, officials and security personnel charged with supervising examinations. Parents are not left out of the business.

Some of these dimensions are discussed below:

(i) **Bringing of Foreign Materials into Examination Hall:** This is a situation where students bring into the examination hall notes, textbooks, and other prepared materials. The method has nicknamed as “hide and seek microchip, tattoo or magic desk”. Sometimes students bring into the hall unauthorized materials like sophisticated and scientific calculators or four figure tables. Some methods like contraband, bullet, super print, escort, missiles, and pregnant biros and so on.

(ii) **Assistance from Educational Stakeholders:** Examination stakeholders include parents, teachers, lecturers, supervisors, security agents, printers and staff of examination bodies. Some parents go to any length in buying question papers for their children while some others even buy certificates for their children. Supervisors colluding with teachers, school principals or students by allowing teachers to come around to teach the students during the examination period; lecturers or teachers releasing question papers, giving underserved marks, or allowing students to illegally re-take examination papers. Security agents, printers and staff of examination bodies also sell question papers.

(iii) **Impersonation:** This is a situation where a candidate sits in an examination for another candidate, thereby pretending to be the real or original candidate. Impersonation is becoming very rampant, even among school candidates.

4.3 The Need for Biometric Technology In Examination Administration

For years the methods used for admitting students to an examination have been very primitive. Either the school authorities used ID cards, Library Cards, fees Clearance Cards or Photo Cards, etc. for authenticating students into an examination hall. However, there were lot of problems faced by the school management in such method such as sometimes the card would be stolen, forgotten at home or even faked in some cases. Also, the traditional method of students using their identity cards to gain entrance into the examination hall after been checked by the supervisors is cumbersome, time consuming and highly insecure as it gives room for impersonation (Folaponmile *et al.*, 2018). With higher institutions in this country increasing their students intake into various programmes each year due to the ever increasing population of the nation, impersonation during exam has also been on the increase, therefore the need to device ways in which to cub this menace. But the good news is that with the use of a multi-mode biometrics which includes (fingerprint software and other biometric identification like face recognition) has brought a solution to the problem of examination malpractice to a great extent in schools.

Biometrics is a technology that (uniquely) identifies a person based on his physiological or behavioral characteristics. Folaponmile *et al.* (2018) said it can be used to achieve a positive identification with a very high level of confidence, such as an error rate of 0.001%. Fingerprint technology using biometrics employs certain advantage of eradicating the problem of examination impersonation by allowing the measure of what you are to perform the security activities of student participation in the examinations.

The use of biometric identification has also lead to increase in efficiency. Instead of serving a long queue for checking the students' I.D before letting students enter an examination room, the biometrics helps schools to avoid backed-up, unauthorized entry, fake I.D. cards. Also the use of biometric devices helps increase security levels of the school and protects the students' privacy. This is because of the simple fact that as against the traditional I.D cards and PINs one student cannot misuse, forge, steal another student's biometric identification in order to access a fellow students' account. These biometric technologies are much reliable, they save the cost of producing cards, easy to use, as well as secure for the students.

4.4 Biometric Systems Adopted in Examinations Administrations

There have been a lot of researches on the adoption of biometric technology in solving the problem of identification of students during examinations. Many biometric systems have also been developed to provide a more secure, faster and easier platform for identification during examination in order to prevent examination malpractices through impersonation. Some of the biometric systems are discussed below.

Ahmed and Abdulaziz (2017) developed a biometric model, which uses fingerprint technology. Their system helps in identifying and verifying student during examinations with a view of minimizing exams malpractice. The introduction of fingerprint based exam verification system was used to easily identify students that registered for a particular course and can easily identify students that are eligible to enter the exam hall. Prototyping software development methodology was adopted, this system was designed using the (Structured System Analysis and Design Methodology) SSADM and Prototype Model which is object-oriented. Visual Basic 6.0 was used to design the interfaces and Mysql was used as the back-end. The system was evaluated using usability testing, and the tests that were carried out include the Test of Biometric Efficiency, Speed of Identification and Authentication, Test of General Requirement. Finally, the system was said to be more secured, more efficient, and had better performance when compared with the manual system of students' verification.

Ekwonwune and Okonkwo (2019) designed a program that addresses issues of examination misconducts such as impersonation and revealed the effectiveness of biometric system using fingerprint in conducting examination clearance. The method that was used involves Structured System Analysis and Methodology (SSADM). The system used fingerprint biometric that compulsorily prompt for biometric (fingerprint) in order to allow students gain access into the system for authentication and identification of the real student before entering into examination hall.

Their Biometric Authentication Approach (BAA) system revealed a more secured, credible and error free to checkmate student malpractices, impersonation and other unlawful acts as compared to existing manual-paper based. The unethical manner associated with the examination is a grim issue that require the stakeholders in academic area to seek for alternative means of authenticating student for examination because, the manual paper-based clearance process is fundamentally flawed (Saheed *et al*., 2017).

In view of this problem Saheed *et al.* (2017) developed a system students' clearance using fingerprint biometrics that addressed the shortcomings of the manual approach. The study adopted a qualitative research method. The model was implemented using Java programming language and the back-end makes use of MySQL as the database as well as the template. SecuGen fingerprint scanner was used to capture live fingerprint image. The system revealed the uniqueness in the use of fingerprint as a reliable access control technique thereby eliminating impersonation in examination and the issue of fake clearance cards.

Oyediran *et al*. (2018) developed an examination authentication embedded system using fingerprints, *a* dependable and effective system that uses fingerprint as biometric modality to tackle the issues of the convectional technique of identification of students before examination. It is a system that allows the students scan their finger in order to gain access into the examination hall. The system works by having each student scan their finger into it while the system cross-check the fingerprint database that was captured during registration to verify if the print is there. The system then grants access by displaying accepted without alarm and if not it sounds an alarm indicating an intruder and displays declined.

The system works with a standalone, handheld and rechargeable device. The system was tested with thirty-six (36) understudied fingerprints. That were enrolled and registered with the system. Each understudied fingerprint was given an ID and the system was able to verify that they were registered. Also, the system was able to identify an unregistered fingerprint and sounds an alarm. The system gives the time when the understudy was verified, and the system generates a report in real time using the understudy fingerprint to avoid or prevent impersonation.

Survey investigation and analysis of the current method of paper-based examination clearance in some higher institutions has the challenge of impersonation of another user with genuine card (Geetha, 2010). Due to the inefficiency of traditional methods of clearance, a more secured and accurate biometric based model was formulated and implemented by Geetha (2010) who to designed a *microsystem embedded system for fingerprint verification*. The system was implemented on the ZF Microsystems based single board computer with Cyrix Media GX based processor and coprocessor with a bus speed of 180MHz. The board supports Windows 3.11, 95/98, and Red Hat Linux 4.0.

Folaponmile *et al.* (2018) observed that the traditional method of students using their Identity cards to gain entrance into the examination hall after been checked by the supervisors is cumbersome, time consuming and highly insecure because it gives room for impersonation. This prompt them to developed an authentication system for students examination in which students biometrics are captured at the point of registration and then used for authentication before the commencement of each examination. The biometric feature used in their system was the fingerprint, their system uses a finger print sensor, arduinouno board, a Bluetooth device, a mobile phone to design a prototype that can be used for students' authentication for examination purposes thereby preventing impersonation in examinations. The system was tested and detected unregistered students, thereby making it more secure and fast in admitting students into the examination hall.

In the view of Ogherohwo and Ezeoba (2016) the menace of examination malpractice in our education system at all levels has compromised the integrity of our educational system, hence the need to have a unique, measurable and universal marker to identify every student for an examination especially in large classes, where facial recognition may not be practical or effective because of the population, thus reducing, or completely eliminating examination malpractice by impersonation.

Ogherohwo and Ezeoba (2016) therefore designed and constructed a biometric device for student authentication during examination using fingerprint for the authentication of the student's eligibility for an examination. After observing from the results obtained in using the device to verify students, and also considering the time taken for the enrollment and verification exercise to be achieved, the biometrics device proved to be effective and reliable way of automatically verifying students for an examination, especially for large classes where facial recognition of every student will not be practical to avoid student impersonation during examination.

Traditional systems to verify a person's identity are based on knowledge (secret code) or possession (ID card), however codes can be forgotten or overheard and ID cards can be lost or stolen giving impostors the possibility to pass the identity test (Vaishnavi, Mangita, Supriya & Dananjay, 2019). In view of these observed challenges, Vaishnavi *et al.* (2019) developed a fingerprint based examination authentication system. It was designed to allow only users verified by their fingerprint scan and does not allow non verified users.

Akintoye *et al.* (2018) noted that the trend in students' examination malpractices comes up with new method year-in-year-out and one of the methods in examination malpractices is impersonation which is one of many challenges schools are facing today in accurately identifying students. They also observed that many models of identification have been adopted, such as picture Identity cards, Personal identification numbers (PINs) in form of matriculation or registration number, and visual identification. Identity cards are often forgotten, damaged, and lost; PINs are easily stolen, forgotten, or swapped, there is misrepresentation using visual identification, particularly in the case of identical twins.

In finding solution to the observed challenges Akintoye *et al*. (2018) designed a students' examination identification scheme based on finger vein pattern that provided an ideal and acceptable solution for accurate identification of students. The finger vein trait is unique for individual and its location under the skin of the finger gives promising pattern for personal identification and authentication. The simulation result of their system showed identification accuracy rate of 92.72%, thus, the scheme was able to prevent impersonation among students during examination.

Olufemi (2010) observed that the major technique for admitting students into an examination over the years has been through the presentation of a token embedded in a physical and portable device which contains the user identity, such devices include ID cards, Library Cards, Fees Clearance Cards, Photo Cards. His observation is that object on these ID tools can be misplaced, stolen, forgotten at home or somewhere, and ID card can also be faked and the advent of both fingerprint scanner and web cam on modern laptop and notebook computers motivated him to developed a multi–mode biometric solution for examination malpractices where fingerprints and face features were used. In his system, there was a fusion of independent information presented by multiple traits (fingerprint and face), that are consolidated and concatenated to compute a new feature vector with higher dimensionality that represents a person's identity in a new hyperspace that affirm the authenticity of the claimed identity.

5. CONCLUSION AND RECOMMENDATIONS

This article has reviewed the concepts of biometric technology and its important use in examination, most especially in curbing to the menace of examination malpractice occasioned by impersonation. Various systems that have been develop in line with the biometric technology for access into examination hall were reviewed to establish their strengths and limitations for further study to improve and enhance the efficiency of biometric technology in the conduct of examinations. The review shows that biometric technology is more secured, credible, and a better substitute for the manual paper-based approach that is known to be characterized with a lot of flaws, irregularities and inefficiencies. However, it was observed that most of the biometric systems adopt single-modality biometric technology, which is not too secure enough for verification, identification and authentication in checkmating examination malpractices and impersonation. This review discloses the several possibilities of future researches taken into consideration some of the limitations of earlier works as presented in this study.

In view of the shortcomings associated with each of the single biometric trait adopted in the reviewed biometric systems, the accuracy, security and efficiency of the biometric technology can be enhanced and improved with the adoption of multimodal (multiple traits) biometric systems. To achieve this, it is recommended that further research be carried out on combination of many biometric traits, such as combination of (fingerprint and face and voice and body odour).

REFERENCES

1. Ahmed, B. A. and Abdulaziz, A. (2017). *Design and Modeling of a Student Verification System in an Examination in Nigeria Using Biometric Fingerprint Technology.* International Journal of Advanced Academic Research, Sciences, Technology & Engineering. ISSN: 2488-9849 Vol. 3, Issue 7.
2. Akintoye, K. A., Araoye, O. I. and Adu, M. K. (2018). *Students Examination Identification Scheme Based on Biometric Finger Vein Pattern.* International Journal of Innovative Research and Development. Vol. 7 Issue 6. *ISSN 2278 – 0211 (Online)* www.ijird.com.
3. Baker, S., Bowyer, K. W. and Flynn, P. J. (2009). Empirical Evidence for Correct Iris Match Score Degradation with Increased Time Lapse between Gallery and Probe Images, *International Conference on Biometrics*, pp. 1170-1179. Available at http://www.nd.edu/~kwb/BakerBowyerFlynnICB_2009.pdf.
4. Danny, T. (2020). *How are Biometric Systems Helping in Curbing Exam Malpractices*? www.bayometric.com.
5. Ekwonwune, E. N. and Okonkwo, T. O. (2019). *A Biometric Authentication Approach to Examination Conduct in Nigerian Universities,* International Journal of Innovative Research in Science, Engineering and Technology, Vol. 8, Issue 3. Available at www.ijirset.com.
6. Folaponmile, A., Okpe, J.B. and Gwani, Y. J. (2018). *Student Examination Attendance Authentication System (SEAAS)*.JORIND 16(1). ISSN 1596-8303. www.transcampus.org/journal; www.ajol.info/journals/jorind.
7. Geetha, M. R. (2010). *ZF Microsystem Based Embedded System Application for Fingerprint Verification.* California: Department of Electrical and Electronic Engineering, California State University, Sacramento.
8. Inbavalli, P. and Nandhini, G. (2014). Body Odor as a Biometric Authentication. International Journal of Computer Science and Information Technologies, (IJCSIT). Vol. 5 (5), 2014, 6270-6274, ISSN: 0975-9646.
9. Jain, A. K., Ross, A. and Prabhakar, S. (2004). *An Introduction to Biometric Recognition*. *IEEE Transactions on Circuits and Systems for Video Technology*, Special Issue on Image and Video-Based Biometrics 14(1).
10. Joseph, N. P. and Lynette, I. M. (2010). *Biometric Recognition: Challenges and Opportunities*. National Academy of Sciences. The National Academies Press 500 Fifth Street, N.W. Washington, DC 20001 ISBN 978-0-309-14207-6. Available at http://www.nap.edu.
11. Ogherohwo E.P. and Ezeoba, E.O. (2016). *Design and Construction of a Biometric Examination Authentication Device.* International Journal of Advanced Research in Physical Science (IJARPS), Volume 3, Issue 5, PP 29-39 ISSN 2349-7874 (Print) & ISSN 2349-7882 (Online) www.arcjournals.org.
12. Olufemi, S. A. (2010). *Multi –Mode Biometric Solution for Examination Malpractices in Nigerian Schools.* International Journal of Computer Applications (0975 – 8887). Volume 4, No. 7.
13. Olufemi, S. A. (2010). A Survey of Emerging Biometric Technologies. International Journal of Computer Applications. Volume 9, No.10, pg 1-5.
14. Oyediran, M. O., Wahab, W. B., Elegbede, A. W. and Enegbe, T. J. (2018). *Development of An Examination Authentication Embedded System Based on Fingerprint Approach.* International Journal of Computers & Technology, Volume: 17 Issue: 1, ISSN: 2277-3061.
15. Oyeleye, C. A., Fagbola, T. M., Babatunde, R. S., and Adigun, A. A. (2012). An Exploratory Study of Odor Biometrics Modality for Human Recognition. International Journal of Engineering Research & Technology (IJERT). Vol. 1 Issue 9. ISSN: 2278-0181. Available at www.ijert.org

16. Ross, A. and Jain, A.K. (2004). Multimodal Biometrics: An Overview. Proceedings of 12th European Signal Processing Conference. http://biometrics.cse.msu.edu/Publications/Multibiometrics/RossJain _MultimodalOverview_EUSIPCO04.pdf
17. Saheed, Y. K., Hambali, M. A., Adeniji, I. A. and Kadri, A. F. (2017). *Fingerprint Based Approach for Examination Clearance in Higher Institutions.* FUOYE Journal of Engineering and Technology. Volume 2, Issue 1. ISSN: 2579-0625 (Online), 2579-0617 (Paper).
18. Vaishnavi, V. K., Mangita, S. W., Supriya, K. G. and Dananjay, B. S. (2019). Fingerprint Based Exam Hall Authentication. International Journal of Research in Engineering, Science and Management Volume-2, Issue-10, October-2019 www.ijresm.com. ISSN (Online): 2581-5792.